UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
SEATTLE DIVISION

VEERA DARUWALLA, MICHAEL MARCH, and LAVICIEIA STURDIVANT, individually and on behalf of classes of similarly situated individuals,

Plaintiffs,

v.

T-MOBILE USA, INC.

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Violation of the California Consumer Privacy Act § 1798.150
(2) Negligence
(3) Negligence *Per Se*
(4) Unjust Enrichment
(5) Breach of Implied Contract
(6) Breach of Confidence
(7) Declaratory and Injunctive Relief

DEMAND FOR JURY TRIAL

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiffs Veera Daruwalla, Michael March, and Lavicieia Sturdivant ("Plaintiffs"), individually and on behalf of classes of similarly situated individuals (defined below), bring this action against Defendant T-Mobile USA, Inc. ("T-Mobile" or "Defendant"). Plaintiffs make the following allegations based upon personal knowledge as to their own actions and upon information and belief as to all other matters and believe that reasonable discovery will provide additional evidentiary support for the allegations herein.

I. NATURE OF THE CASE

1. "Not all data breaches are created equal. None of them are good, but they do come in varying degrees of bad. And given how regularly they happen, it's understandable that you may have become inured to the news. Still, a T-Mobile breach that hackers claim involved the data of 100 million people deserves your attention…." WIRED Magazine, *The T-Mobile Data Breach is One You Can't Ignore,* August 16, 2021.

2. On the same day that article was printed, T-Mobile confirmed that hackers using the Twitter handle ***@und0xxed*** had in fact gained unauthorized access to T-Mobile data through T-Mobile servers (the "Data Breach").

3. According to the hackers, the stolen personal identifying information ("PII") includes customers' names, addresses, social security numbers, drivers license information, phone numbers, dates of birth, security PINs, phone numbers, and, for some customers, unique IMSI and IMEI numbers (embedded in customer mobile devices that identify the device and the SIM card that ties that customer's device to a telephone number)—all going back as far as the mid 1990s. The hackers also claim to have a database that includes credit card numbers with six digits of the cards obfuscated.

4. As the WIRED article points out: "[T]he apparent T-Mobile breach offers potential buyers a blend of data that could be used to great effect." "[H]aving [this PII] centralized streamlines the [identity theft] process for criminals…" And while it may be true

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

that "names and phone numbers are relatively easy to find … a database that ties those two together, along with identifying someone's carrier and fixed address, makes it much easier to convince someone to click on a link that advertises, say, a special offer or upgrade for T-Mobile customers. And to do so en masse."

5. Furthermore, "[b]ecause each IMEI number is tied to a specific customer's phone, knowing it could help in a so-called SIM-swap attack" which "could lead to account takeover concerns…since threat actors could gain access to two-factor authentication or one-time passwords tied to other accounts—such as email, banking, or any other account employing advanced authentication security feature—using a victim's phone number." In fact, a previous T-Mobile data breach disclosed in February of this year—one of many it has suffered in the last few years—was used specifically to execute a SIM-swap attack.[1]

6. According to the hackers, the Data Breach reportedly affects more than 100 million individuals, meaning that all or nearly all T-Mobile customers may have been impacted.[2] As of August 18, T-Mobile has conceded that its "preliminary investigation" indicates that at *least* 7.8 million current T-Mobile postpaid customer accounts were in the stolen files, as well as over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile, 850,000 active prepaid customers, and some additional information from inactive prepaid accounts access through prepaid billing files. The investigation appears ongoing and therefore may reveal additional affected accounts.

[1] *See, e.g.*, Gatlan, Sergio, *T-Mobile discloses data breach after SIM swapping attacks,* Bleeping Computer, Feb. 26, 2021, available at https://www.bleepingcomputer.com/news/security/t-mobile-discloses-data-breach-after-sim-swapping-attacks/.

[2] T-Mobile US Inc. (2020). Form 10-K 2020 at 5. Retrieved from https://www.sec.gov/ix?doc=/Archives/edgar/data/0001283699/000128369921000039/tmus-20201231.htm.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

7. But while T-Mobile has confirmed that a breach occurred, it has yet to provide any notice or instruction to its customers, other than that "communications will be issued shortly" recommending that all T-Mobile postpaid customers proactively change their PIN and take advantage of Account Takeover Protection capabilities. Unfortunately, it is too late: according to the hackers, they have already sold a first batch containing hundreds of thousands of records and are shopping the bulk of the stolen PII directly to buyers.

8. As the target of many data breaches in the past, T-Mobile knew its systems were vulnerable to attack. Yet it failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect its customers' personal information, yet again putting millions of customers at great risk of scams and identity theft. Its customers expected and deserved better from the second largest wireless provider in the country.

9. The customer PII disclosed in the Data Breach is protected by the California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.100 ("CCPA"), which gives rise to a cause of action when insufficient security results in a breach. Specifically, the CCPA gives rise to a claim where, as here, an individual's name in combination with a social security number or driver's license number are exfiltrated without authorization (among other things).[3]

10. In a private right of action, the CCPA also provides for statutory damages of between $100 and $750 per customer per violation or actual damages, whichever is greater. The appropriate amount of statutory damages is determined through examination of a number of factors, including the size of Defendant's assets and whether the Defendant has a record of weak data security.

[3] In other sections of the CCPA, "personal information" is defined more broadly as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

11. Finally, the CCPA provides that "[a]ny provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this title, including, but not limited to, any right to a remedy or means of enforcement, shall be deemed contrary to public policy and shall be void and unenforceable."

12. Plaintiffs now seek compensation under the CCPA and principles of common law negligence, unjust enrichment, breach of implied contract, and breach of confidence, for their damages and those of fellow class members. Plaintiffs also seek injunctive relief to ensure that T-Mobile cannot continue to put its customers at risk.

II. JURISDICTION AND VENUE

13. This Court has jurisdiction over this action under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and one or more members of the classes are residents of a different state than the Defendant. The Court also has supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

14. This Court has personal jurisdiction over Defendant because it is headquartered in this District.

15. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(b) and (c) and 15 U.S.C. §§ and 22, as Defendant resides, transacts business, committed an illegal or tortious act, has an agent, and/or can be found in this District.

III. PARTIES

16. Plaintiff Veera Daruwalla is a resident of Kern County, California. As a current T-Mobile customer since at least 2018, Ms. Daruwalla believes her PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach.

17. Plaintiff Michael March is a resident of Chalmette, Louisiana and was a T-Mobile customer for approximately eight years before canceling his services due to privacy

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

concerns. As a former T-Mobile customer, Mr. March believes his PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach.

18. Plaintiff Lavicieia Sturdivant is a resident of Evanston, Illinois and has been a T-Mobile customer for approximately 18 years. On August 19, 2021, Ms. Sturdivant received a text message from T-Mobile notifying her that her PII was accessed without authorization, exfiltrated, and/or stolen in the Data Breach.

19. Defendant, T-Mobile USA, Inc., is a Delaware corporation headquartered in this district, at 12920 Southeast 38th Street, Bellevue, WA 98006. Defendant is a publicly traded company organized and operated for the profit and financial benefit of its shareholders. As of January 1, 2021, Defendant had annual gross revenues of well over $60 billion. Defendant collects and maintains the personal information of millions of U.S. and California consumers.

20. Defendant's unlawful conduct was authorized, ordered, or performed by its directors, officers, managers, agents, employees, or representatives in the course of their employment and while actively engaged in the management of Defendant's affairs. Defendant, through its subsidiaries, divisions, affiliates and agents, operated as a single unified entity with each acting as the alter ego, agent or joint-venturer of or for the other with respect to the acts, violations, and common course of conduct alleged herein and under the authority and apparent authority of parent entities, principals and controlling parties.

IV. FACTS

The Data Breach

21. As outlined above, T-Mobile has admitted it was the subject of a yet another massive data breach that affected millions of its customers. The customer PII the hackers have sold and continue to market for sale is believed to include: customers' names, addresses, social security numbers, drivers license information, phone numbers, dates of birth, security PINs, phone numbers, and, for some customers, unique IMSI and IMEI numbers (embedded in

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

customer mobile devices that identify the device and the SIM card that ties that customer's device to a telephone number)—all going back as far as the mid 1990s.

22. According to the hackers, they were able to access the PII through an opening in T-Mobile's wireless data network that allowed access to two of T-Mobile's customer data centers. From there, they were able to access several customer databases totaling more than 100 gigabytes.

23. Motherboard, the tech news division of Vice, has reported that it reviewed samples of the data and confirmed it contained accurate information about T-Mobile customers. The hackers also offered to verify that they possessed the customers' PII, stating: "If you want to verify that I have access to the data/the data is real, just give me a T-Mobile number and I'll run a lookup for you and return the IMEI and IMSI of the phone currently attached to the number and any other details," @und0xxed said. "All T-Mobile USA prepaid and postpaid customers are affected; Sprint and the other telecoms that T-Mobile owns are unaffected."

24. As a result of the Data Breach and because the stolen data is being active marketed for sale, numerous entities are suggesting that affected consumers take steps to protect their identities.

25. The Washington Post reported that affected individuals should: 1) Change your password and PIN; 2) freeze your credit; 3) rethink two-factor authentication; and 4) keep monitoring the situation.[4]

[4] Velazco, Chris, *Here's what to do if you think you're affected by T-Mobile's big data breach*, Washington Post, August 19, 2021, available at https://www.washingtonpost.com/technology/2021/08/19/t-mobile-data-breach-what-to-do/

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

T-Mobile Has Failed to Secure its Sensitive Data Numerous Times Over the Last Decade

26. T-Mobile is no stranger to data breaches. Rather, data breaches have been a nearly annual event for the company for many years.

27. The Washington Post reported that "[u]nfortunately, dealing with data breaches is nothing new for the company — or its customers. For those keeping count, this is the fifth such incident the wireless carrier has suffered in the past three years, but according to Allie Mellen, a security and risk analyst at Forrester Research, this is 'the worst breach they've had so far.'"[5]

28. In March **2020**, T-Mobile disclosed it was subject to a data breach that exposed customer and employee PII, including names, addresses, social security numbers, financial account information, government identification numbers, phone numbers and billing account information.[6] Later in 2020, T-Mobile suffered another data breach in which hackers accessed customer proprietary network information (CPNI) and undisclosed call-related information for hundreds of thousands of customers.[7]

---

[5] *Id.*

[6] *T-Mobile Breach Leads To The Exposure Of Employee Email Accounts And User Data*, Identity Theft Resource Center, Mar. 2020, available at https://www.idtheftcenter.org/t-mobile-breach-leads-to-the-exposure-of-employee-email-accounts-and-user-data/#:~:text=On%20Thursday%2C%20March%204%2C%202020%2C%20T-Mobile%20disclosed%20a,separate%20data%20breach%20notification%20letters%20on%20their%20website.

[7] *Second Data Breach in 2020 for T-Mobile Exposed Customer and Call-Related Information of 200,000 Subscribers*, CPO Magazine, Jan. 11, 2021, available at https://www.cpomagazine.com/cyber-security/second-data-breach-in-2020-for-t-mobile-exposed-customer-and-call-related-information-of-200000-subscribers/#:~:text=T-Mobile%20suffered%20a%20data%20breach%20in%20which%20hackers,the%20fourth%20to%20hit%20the%20company%20since%202018.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

29. In November **2019**, hackers accessed PII for roughly 1 million T-Mobile prepaid customers.[8] The PII in that breach included names, phone numbers, addresses, account information, and rate, plan and calling features (i.e., paying for international calls).[9]

30. In **2018**, hackers gained access to T-Mobile servers and stole PII of roughly two million T-Mobile customers.[10] The stolen PII included names, email addresses, account numbers, other billing information, and encrypted passwords.[11] T-Mobile misleadingly downplayed the hack, claiming that no passwords were "compromised."[12] In truth, the hackers stole millions of encrypted passwords that were likely cracked due to the weak encoding algorithm employed by T-Mobile, leading one security expert to advise affected customers to assume their passwords were cracked and change them as a result.[13]

31. In **2017**, Karan Saini, a security researcher, found a bug on a T-Mobile website that allowed hackers to access PII like email addresses, account numbers, and IMSI numbers, just by knowing or guessing a customer's phone number.[14] According to Saini, "T-Mobile has 76 million customers, and an attacker could have ran a script to scrape the data (email, name, billing account number, IMSI number, other numbers under the same account which are

---

[8] Coldeway, Devin, *More than 1 million T-Mobile customers exposed by breach*, TechCrunch, Nov. 22, 2019, available at https://techcrunch.com/2019/11/22/more-than-1-million-t-mobile-customers-exposed-by-breach/#:~:text=More%20than%201%20million%20T-Mobile%20customers%20exposed%20by,password%20data%29%20was%20exposed%20to%20a%20malicious%20actor.

[9] *Id.*

[10] Franceschi-Bicchierai, Lorenzo, *Hackers Stole Personal Data of 2 Million T-Mobile Customers*, Motherboard Tech, Aug, 23, 2018, available at https://www.vice.com/en/article/a3qpk5/t-mobile-hack-data-breach-api-customer-data.

[11] *Id.*

[12] *Id.*

[13] *Id.*

[14] Franceschi-Bicchierai, Lorenzo, *T-Mobile Website Allowed Hackers to Access Your Account Data With Just Your Phone Number*, Motherboard Tech, Oct. 10, 2017, available at https://www.vice.com/en/article/wjx3e4/t-mobile-website-allowed-hackers-to-access-your-account-data-with-just-your-phone-number.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

usually family members) from all 76 million of these customers to create a searchable database with accurate and up-to-date information of all users."[15] Saini explained "[t]hat would effectively be classified as a very critical data breach, making every T-Mobile cell phone owner a victim."[16] T-Mobile had no mechanism in place to prevent this type of critical data breach, according to Saini.[17] According to a hacker, the bug had been exploited by multiple hackers over a multi-week period before it was discovered by Saini.[18] In fact, the hackers who found the bug before Saini went so far as to upload a tutorial on how to exploit it on YouTube.[19]

32. And in **2015**, T-Mobile customers' PII was accessed and exfiltrated in conjunction with the Experian data breach. According to T-Mobile at the time, the company was notified by Experian, a vendor that processes their credit applications, that they had experienced a data breach. The hacker acquired the records of approximately 15 million people, including new applicants requiring a credit check for service or device financing. The records stolen included information such as name, address and birthdate as well as encrypted fields with Social Security number and ID number (such as driver's license or passport number), and additional information used in T-Mobile's own credit assessment. Experian determined that encryption may have been compromised.[20]

---

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Id.*

[20] *A Letter from CEO John Legere on Experian Data Breach*, Sept. 30, 2015, available at https://www.t-mobile.com/news/blog/experian-data-breach

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Defendant's Relevant Privacy Policies

33. T-Mobile's Privacy Policy is available on its website and provides customers with terms and conditions regarding the treatment of their PII, including how T-Mobile uses customers' data for its own benefit and profit.

34. For example, it states T-Mobile uses customers' personal data to **"***[a]dvertise and market products and services from T-Mobile and other companies* to you, including through targeted advertising and communications about promotions and events, contents, and sweepstakes"; and "[c]onduct research and create reports from analysis of things like usage patterns and trends and deidentify or aggregate personal data to *create business and market analysis and reports*."

35. The policy, dated May 5, 2021, also states: "[S]tarting on April 26, 2021, T-Mobile began "*using some data we have about you, including information we learn from your web and device usage data (like the apps installed on your device) and interactions with our products and services, for our own and 3rd party advertising,* unless you tell us not to."

36. According to the policy's California privacy rights section, included for purposes of complying with the CCPA, in the past 12 months T-Mobile has sold to third parties "*shared device identifiers and internet and electronic network activity to facilitate online advertising*. This means that a unique, resettable number that identifies your device was linked to online activity and shared with others who use that data for advertising and analytics purposes (like *advertising networks, data analytics providers, and social media platforms).*"

37. Based on the customer PII T-Mobile collects and sells, T-Mobile states that its customers "*see T-Mobile and other advertisements on your devices - whether you are connected to our network or not. These ads may be targeted to your device based on information that we, the advertiser, and other third parties have about your behavior or interests ….*"

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

38. T-Mobile also "*works with third parties, including advertising networks, which collect information about you through devices, websites, and apps, serve ads for us and others*, and measure their effectiveness. … For example, third parties like Google Ad Manager and Nielsen may use technology to collect data to deliver, personalize, and measure ads for some of our Products and Services. *This technology allows tracking of device activity over time across online properties."*

39. In addition, T-Mobile partners "with *analytic service providers like Google Analytics to help track your use of our products and services.*" "*If your mobile device is turned on, our network is collecting data about where it is.* We may use, provide access to, or disclose this network location data without your permission to provide and support our services."

40. After listing all of these ways T-Mobile benefits and profits from tracking and targeting its customers through collecting and maintaining their invaluable PII, T-Mobile's Privacy Policy goes on to ensure its customers that their PII is secure, stating that (i) *personal data will be disclosed only* "*with your consent,* which we may get in writing, online, or orally," and (ii) T-Mobile uses "*administrative, technical, contractual, and physical safeguards designed to protect your data* while it is under our control." Yet again, those safeguards have failed.

Plaintiff Veera Daruwalla

41. Plaintiff Veera Daruwalla has been a customer of T-Mobile from approximately 2018 through the present, and is a resident of Bakersfield, California.

42. On approximately August 17, 2021, Ms. Daruwalla became aware that that T-Mobile had suffered a massive data breach and customer PII was being sold by hackers. Since then, she has spent hours addressing the resulting privacy concerns, including researching the nature of the breach, and reviewing his financial and credit account statements for evidence of unauthorized activity, which she will continue to do for years into the future.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiff Michael March

43. Plaintiff Michael March is a former T-Mobile customer who resides in Chalmette, Louisiana.

44. Mr. March was a customer of T-Mobile from approximately 2013 through early August 2021.

45. On approximately August 8, 2021, Mr. March visited a T-Mobile store located at 8700 W. Judge Perez Drive in Chalmette, Louisiana to raise concerns about privacy issues he had been experiencing with his T-Mobile account. Specifically, Mr. March believed that someone gained access to his T-Mobile account without authorization. The T-Mobile representative working at the store was dismissive of Mr. March's concerns.

46. On approximately August 10, 2021, Mr. March visited the same T-Mobile store to cancel his account due to the privacy concerns he raised with T-Mobile two days prior. The following week, Mr. March learned through news reports that T-Mobile had suffered a massive data breach and customer data was being sold on underground websites.

47. Mr. March has spent numerous hours communicating with T-Mobile representatives about his privacy concerns, canceling his T-Mobile service and switching to a different cellular service provider, researching the nature of the breach, and reviewing his financial and credit account statements for evidence of unauthorized activity, which he will continue to do for years into the future.

Plaintiff Lavicieia Sturdivant

48. Plaintiff Lavicieia Sturdivant is a current T-Mobile customer who resides in Evanston, Illinois.

49. Ms. Sturdivant has been a customer of T-Mobile for approximately 18 years.

50. On August 19, 2021, received a text message from T-Mobile informing her that her PII was compromised in the Data Breach. Specifically, the text message stated that "T-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Mobile has determined that unauthorized access to some of your personal data has occurred. We have no evidence that debit/credit card information was compromised. We take the protection our customers seriously. We are taking actions to protect your T-Mobile account and we recommend that you take action to protect your credit. Read more here: t-mo.co/Protect".

51. Receiving this message caused Ms. Sturdivant immediate distress as she is in the process of closing on a home and justifiably concerned that she could be the victim of identity theft or fraud. T-Mobile's message also created more questions than it answered. It did not explain the nature of the attack, the identity of the hackers, what information was compromised for Ms. Sturdivant, or the fact that the information had already been released and listed for sale on the dark web. T-Mobile's decision to withhold these key facts is significant because affected individuals may take different precautions depending on the severity and imminence of the perceived risk. By failing to provide these material facts, T-Mobile prevented victims from taking meaningful, proactive, and targeted mitigation measures that could help protect them from years of harm.

52. As a result of the data breach and T-Mobile's deficient notice, Ms. Sturdivant has spent time and effort conducting her own research into the breach and reviewing her financial and credit account statements for evidence of unauthorized activity, which she will continue to do for years into the future. Ms. Sturdivant has also suffered emotional distress knowing that her information is now available for sale and can be used to commit blackmail, extortion, identity theft or fraud, and any number of additional harms against her for the rest of her life.

FTC Security Guidelines Concerning PII

53. The Federal Trade Commission ("FTC") has established security guidelines and recommendations to help entities protect PII and reduce the likelihood of data breaches.

54. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted by the FTC, failing to use reasonable measures

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to protect PII by companies like Defendant. Several publications by the FTC outline the importance of implementing reasonable security systems to protect data. The FTC has made clear that protecting sensitive customer data should factor into virtually all business decisions.

55. In 2016, the FTC provided updated security guidelines in a publication titled *Protecting Personal Information: A Guide for Business*. Under these guidelines, companies should protect consumer information they keep; limit the sensitive consumer information they keep; encrypt sensitive information sent to third parties or stored on computer networks; identify and understand network vulnerabilities; regularly run up-to-date anti-malware programs; and pay particular attention to the security of web applications – the software used to inform visitors to a company's website and to retrieve information from the visitors.

56. The FTC recommends that businesses do not maintain payment card information beyond the time needed to process a transaction; restrict employee access to sensitive customer information; require strong passwords be used by employees with access to sensitive customer information; apply security measures that have proven successful in the particular industry; and verify that third parties with access to sensitive information use reasonable security measures.

57. The FTC also recommends that companies use an intrusion detection system to immediately expose a data breach; monitor incoming traffic for suspicious activity that indicates a hacker is trying to penetrate the system; monitor for the transmission of large amounts of data from the system; and develop a plan to respond effectively to a data breach in the event one occurs.

58. The FTC has brought several actions to enforce Section 5 of the FTC Act. According to its website:

> When companies tell consumers they will safeguard their personal information, the FTC can and does take law enforcement action to make

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

> sure that companies live up these promises. The FTC has brought legal actions against organizations that have violated consumers' privacy rights, or misled them by failing to maintain security for sensitive consumer information, or caused substantial consumer injury. In many of these cases, the FTC has charged the defendants with violating Section 5 of the FTC Act, which bars unfair and deceptive acts and practices in or affecting commerce. In addition to the FTC Act, the agency also enforces other federal laws relating to consumers' privacy and security.

59. T-Mobile was aware or should have been aware of its obligations to protect its customers' PII and privacy before and during the Data Breach yet failed to take reasonable steps to protect customers from unauthorized access. Among other violations, T-Mobile violated its obligations under Section 5 of the FTC Act.

The Data Breach Harmed Plaintiffs and Class Members

60. Plaintiffs and Class members have suffered and will continue to suffer harm because of the Data Breach.

61. Plaintiffs and Class members face an imminent and substantial risk of injury of identity theft and related cyber crimes due to the Data Breach. Once data is stolen, malicious actors will either exploit the data for profit themselves or sell the data on the dark web, as occurred here, to someone who intends to exploit the data for profit. Hackers would not incur the time and effort to steal PII and then risk prosecution by listing it for sale on the dark web if the PII was not valuable to malicious actors.

62. The dark web helps ensure users' privacy by effectively hiding server or IP details from the public. Users need special software to access the dark web. Most websites on the dark web are not directly accessible via traditional searches on common search engines and are therefore accessible only by users who know the addresses for those websites.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

63. Malicious actors use PII to gain access to Class members' digital life, including bank accounts, social media, and credit card details. During that process, hackers can harvest other sensitive data from the victim's accounts, including personal information of family, friends, and colleagues.

64. Malicious actors can also use Class members' PII to open new financial accounts, open new utility accounts, obtain medical treatment using victims' health insurance, file fraudulent tax returns, obtain government benefits, obtain government IDs, or create "synthetic identities."

65. The PII accessed in the Data Breach therefore has significant value to the hackers that have already sold or attempted to sell that information and may do so again. In fact, names, mailing and email addresses, dates of birth, phone numbers, account information, social security numbers, phone identification numbers, and drivers license numbers are among the most valuable pieces of information for hackers.

66. As established above, the PII accessed in the Data Breach is also very valuable to T-Mobile. T-Mobile collects, retains, and uses this information to increase profits through predictive and other targeted marketing campaigns. T-Mobile customers value the privacy of this information and expect T-Mobile to allocate enough resources to ensure it is adequately protected. Customers would not have done business with T-Mobile, provided their PII and payment card information, and/or paid the same prices for T-Mobile's goods and services had they known T-Mobile did not implement reasonable security measures to protect their PII. T-Mobile boasts that it is the second largest wireless carrier in the country. Customers expect that the payments they make to the carrier, either prepaid or each month, incorporate the costs to implement reasonable security measures to protect customers' personal information.

67. The PII accessed in the Data Breach is also very valuable to Plaintiffs and Class members. Consumers often exchange personal information for goods and services. For

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

example, consumers often exchange their personal information for access to wifi in places like airports and coffee shops. Likewise, consumers often trade their names and email addresses for special discounts (*e.g.*, sign-up coupons exchanged for email addresses). Consumers use their unique and valuable PII to access the financial sector, including when obtaining a mortgage, credit card, or business loan. As a result of the Data Breach, Plaintiffs and Class members' PII has been compromised and lost significant value.

68. Plaintiffs and Class members will face a risk of injury due to the Data Breach for years to come. Malicious actors often wait months or years to use the personal information obtained in data breaches, as victims often become complacent and less diligent in monitoring their accounts after a significant period has passed. These bad actors will also re-use stolen personal information, meaning individuals can be the victim of several cyber crimes stemming from a single data breach. Finally, there is often significant lag time between when a person suffers harm due to theft of their PII and when they discover the harm. For example, victims rarely know that certain accounts have been opened in their name until contacted by collections agencies. Plaintiffs and Class members will therefore need to continuously monitor their accounts for years to ensure their PII obtained in the Data Breach is not used to harm them.

69. Even when reimbursed for money stolen due to a data breach, consumers are not made whole because the reimbursement fails to compensate for the significant time and money required to repair the impact of the fraud. On average, victims of identity theft spend 7 hours fixing issues caused by the identity theft. In some instances, victims spend more than 1,000 hours trying to fix these issues.

70. Victims of identity theft also experience harm beyond economic effects. According to a 2018 study by the Identity Theft Resource Center, 32% of identity theft

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

victims experienced negative effects at work (either with their boss or coworkers) and 8% experienced negative effects at school (either with school officials or other students).

71. The U.S. Government Accountability Office likewise determined that "stolen data may be held for up to a year or more before being used to commit identity theft," and that "once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years."

72. Plaintiffs and Class Member customers have failed to receive the value of the T-Mobile services for which they paid and/or would have paid less had they known that T-Mobile was failing to use reasonable security measures to secure their data.

Defendant Failed to Take Reasonable Steps to Protect its Customers' PII

73. T-Mobile requires its customers to provide a significant amount of highly personal and confidential PII to purchase its good and services. Defendant collects, stores, and uses this data to maximize profits while failing to encrypt or protect it properly.

74. T-Mobile has legal duties to protect its customers' PII by implementing reasonable security features. This duty is further defined by federal and state guidelines and industry norms.

75. Defendant breached its duties by failing to implement reasonable safeguards to ensure Plaintiffs' and Class members' PII was adequately protected. As a direct and proximate result of this breach of duty, the Data Breach occurred, and Plaintiffs and Class members were harmed. Plaintiffs and Class members did not consent to having their PII disclosed to any third-party, much less a malicious hacker who would sell it to criminals on the dark web.

76. The Data Breach was a reasonably foreseeable consequence of Defendant's inadequate security systems. T-Mobile, which made approximately $70 billion in revenue in 2020, certainly has the resources to implement reasonable security systems to prevent or limit damage from data breaches. And after almost yearly data breaches for the past 5 years, it knew

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

that its systems were utterly lacking. Even so, it failed to properly invest in its data security. Had T-Mobile implemented reasonable data security systems and procedures (*i.e.*, followed guidelines from industry experts and state and federal governments), then it likely could have prevented hackers from infiltrating its systems and accessing its customers' PII.

77. T-Mobile's failure to implement reasonable security systems has caused Plaintiffs and Class members to suffer and continue to suffer harm that adversely impact Plaintiffs and Class members economically, emotionally, and/or socially. As discussed above, Plaintiffs and Class members now face a substantial, imminent, and ongoing threat of identity theft, scams, and resulting harm. These individuals now must spend significant time and money to continuously monitor their accounts and credit scores and diligently sift out phishing communications to limit potential adverse effects of the Data Breach regardless of whether any Class member ultimately falls victim to identity theft.

78. In sum, Plaintiffs and Class members were injured as follows: (i) theft of their PII and the resulting loss of privacy rights in that information; (ii) improper disclosure of their PII; (iii) the lost value of unauthorized access to their PII; (iv) diminution in value of their PII; (v) the certain, imminent, and ongoing threat of fraud and identity theft, including the economic and non-economic impacts that flow therefrom; (vi) ascertainable out-of-pocket expenses and the value of their time allocated to fixing or mitigating the effects of the Data Breach; (vii) overpayments to T-Mobile for goods and services purchased, as Plaintiffs and Class members reasonably believed a portion of the sale price would fund reasonable security measures that would protect their PII, which was not the case; and/or (viii) nominal damages.

79. Even though T-Mobile has decided to offer free credit monitoring for two years to its affected customers, this is insufficient to protect Plaintiffs and Class members. As discussed above, the threat of identity theft and fraud from the Data Breach will extend for many years and cost Plaintiffs and the Classes significant time and effort. Although it has not

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

yet notified all individual customers of the breach, T-Mobile's website acknowledges this, encouraging customers to postpaid customers proactively change their PIN and take advantage of Account Takeover Protection capabilities.

80. Plaintiffs and Class members therefore have a significant and cognizable interest in obtaining injunctive and equitable relief (in addition to any monetary damages) that protects them from these long-term threats. Accordingly, this action represents the enforcement of an important right affecting the public interest and will confer a significant benefit on the general public or a large class of persons.

VI. CLASS ACTION ALLEGATIONS

81. Plaintiffs bring this action on behalf of themselves and all others similarly situated pursuant to Federal Rule of Civil Procedure 23 as representative of the Classes defined as follows:

(a) **The Nationwide Class:** All U.S. residents whose data was exfiltrated in the Data Breach.

(b) **The California Class:** All California residents whose data was exfiltrated in the Data Breach.

82. Specifically excluded from the Classes are Defendant; its officers, directors, or employees; any entity in which Defendant has a controlling interest; and any affiliate, legal representative, heir, or assign of Defendant. Also excluded from the Classes are any federal, state, or local governmental entities, any judicial officer presiding over this action and the members of their immediate family and judicial staff, and any juror assigned to this action.

83. Class Identity: The members of the Classes are readily identifiable and ascertainable. Defendants and/or their affiliates, among others, possess the information to identify and contact class members.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

84. Numerosity: The members of the Classes are so numerous that joinder of all of them is impracticable. While the exact number of class members is unknown to Plaintiffs at this time, based on information and belief, the Nationwide Class consists of between 50 and 100 million customers whose data was compromised in the Data Breach, and the California Class consists of millions of customers whose data was compromised in the Data Breach.

85. Typicality: Plaintiffs' claims are typical of the claims of the members of the classes because all class members had their PII accessed, exfiltrated, and stolen in the Data Breach and were harmed as a result.

86. Adequacy: Plaintiffs will fairly and adequately protect the interests of the Classes. Plaintiffs have no interest antagonistic to those of the classes and are aligned with Class members' interests because Plaintiffs were subject to the same Data Breach as Class members and faces similar threats due to the Data Breach as Class members. Plaintiffs have also retained competent counsel with significant experience litigating complex class actions, including Data Breach cases involving multiple classes and CCPA claims.

87. Commonality and Predominance: There are questions of law and fact common to the classes. These common questions predominate over any questions affecting only individual class members. The common questions of law and fact include, without limitation:

a. Whether Defendant violated § 1798.150 of the CCPA;

b. Whether Defendant owed Plaintiffs and class members a duty to implement and maintain reasonable security procedures and practices to protect their personal information;

c. Whether Defendant breached an implied contract with Plaintiffs and class members, including but not limited to whether Defendant breached an implied agreement with Plaintiffs and class members to keep their PII confidential;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

d. Whether Defendant received a benefit without proper restitution making it unjust for Defendant to retain the benefit without commensurate compensation;

e. Whether Defendant acted negligently in connection with the monitoring and/or protection of Plaintiffs' and class members' PII;

f. Whether Defendant breached its duty to implement reasonable security systems to protect Plaintiffs' and class members' PII;

g. Whether Defendant's breach of its duty to implement reasonable security systems directly and/or proximately caused damages to Plaintiffs and class members;

h. Whether Defendant adequately addressed and fixed the vulnerabilities that enabled the Data Breach;

i. When Defendant learned of the Data Breach and whether its response was adequate;

j. Whether Plaintiffs and other class members are entitled to credit monitoring and other injunctive relief;

k. Whether Defendant provided timely notice of the Data Breach to Plaintiffs and class members; and,

l. Whether class members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach.

88. Defendant has engaged in a common course of conduct and class members have been similarly impacted by Defendant's failure to maintain reasonable security procedures and practices to protect customers' PII, as well as Defendant's failure to timely alert affected customers to the Data Breach.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

89. Superiority: A class action is superior to other available methods for the fair and efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most if not all class members would find the cost of litigating their individual claims prohibitively high and have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members and risk inconsistent treatment of claims arising from the same set of facts and occurrences.

Plaintiffs know of no difficulty likely to be encountered in the maintenance of this action as a class action under Federal Rule of Civil Procedure 23.

VII. CLAIMS FOR RELIEF

COUNT I
Violation of the CCPA, Cal. Civ. Code § 1798.150
(On Behalf of the California Class)

90. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

91. Defendant is a corporation organized or operated for the profit or financial benefit of its owners with annual gross revenues over $70 billion. Defendant collects consumers' PII as defined in Cal. Civ. Code § 1798.140.

92. Defendant violated § 1798.150 of the CCPA by failing to prevent Plaintiffs' and class members' nonencrypted PII from unauthorized access and exfiltration, theft, or disclosure as a result of Defendant's violations of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

93. Defendant has a duty to implement and maintain reasonable security procedures and practices to protect Plaintiffs' and class members' PII. As detailed herein, Defendant failed to do so. As a direct and proximate result of Defendant's acts, Plaintiffs' and class

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

members' PII, including social security numbers, phone numbers, names, addresses, unique IMEI numbers, and drivers license information, was subjected to unauthorized access and exfiltration, theft, or disclosure.

94. Plaintiffs and class members seek injunctive or other equitable relief to ensure Defendant hereinafter adequately safeguards customers' PII by implementing reasonable security procedures and practices. Such relief is particularly important because Defendant continues to hold customers' PII, including Plaintiffs' and class members' PII. Plaintiffs and class members have an interest in ensuring that their PII is reasonably protected, and Defendant has demonstrated a pattern of failing to adequately safeguard this information.

95. Pursuant to Cal. Civ. Code § 1798.150(b), on August 18, 2021, Plaintiffs mailed CCPA notice letter to Defendant's registered service agents via overnight post, detailing the specific provisions of the CCPA that T-Mobile has and continues to violate. If Defendant cannot cure within 30 days, and Plaintiffs believe such cure is not possible under these facts and circumstances, then Plaintiffs intend to promptly amend this Complaint to seek statutory damages as permitted by the CCPA.

Declaratory Judgment

96. As described herein, an actual controversy has arisen and now exists as to whether Defendant implemented and maintained reasonable security procedures and practices appropriate to the nature of the information to protect the personal information under the CCPA.

97. A judicial determination of this issue is necessary and appropriate at this time under the circumstances to prevent further data breaches by Defendant and third parties with similar inadequate security measures.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

COUNT II
Negligence
(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

98. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

99. Defendant owed Plaintiffs and Class members a duty to exercise reasonable care in protecting their PII from unauthorized disclosure or access. Defendant breached its duty of care by failing to implement reasonable security procedures and practices to protect this PII. Among other things, Defendant failed to: (i) implement security systems and practices consistent with federal and state guidelines; (ii) implement security systems and practices consistent with industry norms; (iii) timely detect the Data Breach; and (iv) timely disclose the Data Breach to impacted customers.

100. Defendant knew or should have known that Plaintiffs' and Class members' PII was highly sought after by cyber criminals and that Plaintiffs and class members would suffer significant harm if their PII was stolen by hackers.

101. Defendant also knew or should have known that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiffs and class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs such as passports and driver's licenses.

102. Defendant had a special relationship with Plaintiffs and Class members who entrusted Defendant with several pieces of PII. Defendant's customers were required to provide PII when purchasing or attempting to purchase Defendant's products and services. Plaintiffs and class members were led to believe Defendant would take reasonable precautions

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to protect their PII and would timely inform them if their PII was compromised, which Defendant failed to do.

103. The harm that Plaintiffs and Class members suffered (and continue to suffer) was the reasonably foreseeable product of Defendant's breach of its duty of care. Defendant failed to enact reasonable security procedures and practices, and Plaintiffs and class members were the foreseeable victims of data theft that exploited the inadequate security measures. The PII accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes.

104. But-for Defendant's breach of its duty of care, the Data Breach would not have occurred and Plaintiffs' and class members' PII would not have been stolen and offered for sale by an unauthorized and malicious party.

105. As a direct and proximate result of the Defendant's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII; lost value of unauthorized access to their PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT III
Negligence *Per Se*
(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

106. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

107. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendant of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of Defendant's duty.

108. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

109. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence *per se*.

110. Class members are consumers within the class of persons Section 5 of the FTC Act (and similar state statutes) were intended to protect.

111. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. Indeed, the FTC has pursued over fifty enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm suffered by Plaintiffs and class members.

112. As a direct and proximate result of the Defendant's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of their stolen PII; lost value of unauthorized access to their PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT IV
Unjust Enrichment
(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

113. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

114. Plaintiffs and class members have an interest, both equitable and legal, in the PII about them that was conferred upon, collected by, and maintained by Defendant and that was ultimately stolen in the Data Breach.

115. Defendant was benefitted by the conferral upon it of the PII pertaining to Plaintiffs and class members and by its ability to retain, use, and profit from that information. Defendant understood that it was in fact so benefitted.

116. Defendant also understood and appreciated that the PII pertaining to Plaintiffs and class members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

117. But for Defendant's willingness and commitment to maintain its privacy and confidentiality, that PII would not have been transferred to and entrusted with Defendant.

118. Defendant continues to benefit and profit from its retention and use of the PII while its value to Plaintiffs and class members has been diminished.

119. Defendant also benefitted through its unjust conduct by selling its services for more than those services were worth to Plaintiffs and class members, who would not have applied for or used T-Mobile service plans at all, or at the terms offered by T-Mobile, had they been aware that Defendant would fail to protect their PII.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

120. Defendant also benefitted through its unjust conduct by retaining money that it should have used to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

121. It is inequitable for Defendant to retain these benefits.

122. As a result of Defendant's wrongful conduct as alleged in this Complaint (including, among things, its knowing failure to employ adequate data security measures, its continued maintenance and use of the PII belonging to Plaintiffs and class members without having adequate data security measures, and their other conduct facilitating the theft of that PII), Defendant has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members.

123. Defendant's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compiling and use of Plaintiffs' and class members' PII, while at the same time failing to maintain that information secure from intrusion and theft by hackers and identity thieves.

124. Under the common law doctrine of unjust enrichment, it is inequitable for Defendant to be permitted to retain the benefits it received, and is still receiving, without justification, from Plaintiffs and class members in an unfair and unconscionable manner. Defendant's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

125. The benefits conferred upon, received, and enjoyed by Defendant was not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

126. Plaintiffs have no adequate remedy at law.

127. Defendant is therefore liable to Plaintiffs and class members for restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

conduct, including specifically: the value to Defendant of the PII that was stolen in the Data Breach; the profits Defendant is receiving from the use of that information; the amounts that T-Mobile overcharged Plaintiffs and class members for use of its services; and the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiffs' and class members' PII.

COUNT V
Breach of Implied Contract
(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

128. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

129. Plaintiffs and class members entered into an implied contract with T-Mobile when they sought or obtained services from T-Mobile, or otherwise provided PII to T-Mobile.

130. As part of these transactions, T-Mobile agreed to safeguard and protect the PII of Plaintiffs and class members, and in the alternative, nominal damages.

131. Plaintiffs and class members entered into implied contracts with the reasonable expectation that T-Mobile's data security practices and policies were reasonable and consistent with industry standards. Plaintiffs and class members believed that T-Mobile would use part of the monies paid to T-Mobile under the implied contracts to fund adequate and reasonable data security practices.

132. Plaintiffs and class members would not have provided and entrusted their PII to T-Mobile or would have paid less for T-Mobile's services in the absence of the implied contract or implied terms between them and T-Mobile. The safeguarding of the PII of Plaintiffs and class members was critical to realize the intent of the parties.

133. Plaintiffs and class members fully performed their obligations under the implied contracts with T-Mobile.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

134. T-Mobile breached its implied contracts with Plaintiffs and class members to protect their PII when it (1) failed to have security protocols and measures in place to protect that information; and (2) disclosed that information to unauthorized third parties.

135. As a direct and proximate result of T-Mobile's breach of implied contract, Plaintiffs and class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid and were overcharged by T-Mobile for its services.

COUNT VI
Breach of Confidence
(On Behalf of the Nationwide Class or Alternatively State-Specific Subclasses)

136. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

137. At all times during Plaintiffs' and class members' interactions with T-Mobile, T-Mobile was fully aware of the confidential and sensitive nature of Plaintiffs' and class members' PII.

138. T-Mobile's relationship with Plaintiffs and class members was governed by terms and expectations that Plaintiffs' and class members' protected PII would be collected, stored, and protected in confidence, and would not be disclosed to the public or any unauthorized third parties.

139. Plaintiffs and class members provided their respective PII to T-Mobile with the explicit and implicit understandings that T-Mobile would protect and not permit the PII to be disseminated to the public or any unauthorized parties.

140. Plaintiffs and class members also provided their respective PII to T-Mobile with the explicit and implicit understandings that T-Mobile would take precautions to protect the PII from unauthorized disclosure, such as following basic principles of encryption and information security practices.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

141. T-Mobile voluntarily received in confidence Plaintiffs' and class members' PII with the understanding that PII would not be disclosed or disseminated to the public or any unauthorized third parties.

142. Due to T-Mobile's failure to prevent, detect, avoid the Data Breach from occurring by following best information security practices to secure Plaintiffs' and class members' PII, Plaintiffs' and class members' PII was disclosed and misappropriated to the public and unauthorized third parties beyond Plaintiffs' and class members' confidence, and without their express permission.

143. But for T-Mobile's disclosure of Plaintiffs' and class members' PII in violation of the parties' understanding of confidence, their PII would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. The Data Breach was the direct and legal cause of the theft of Plaintiffs' and class members' PII, as well as the resulting damages.

144. The injury and harm Plaintiffs and class members suffered was the reasonably foreseeable result of T-Mobile's unauthorized disclosure of Plaintiffs' and class members' PII. T-Mobile knew its computer systems and technologies for accepting, securing, and storing Plaintiffs' and class members' PII had serious security vulnerabilities because T-Mobile failed to observe even basic information security practices or correct known security vulnerabilities.

145. As a direct and proximate result of T-Mobile's breaches of confidence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen PII; illegal sale of the compromised PII on the black market; mitigation expenses and time spent on

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their PII; lost value of unauthorized access to their PII; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT VII
Declaratory Judgment
(On Behalf of the Nationwide Class)

146. Plaintiffs repeat and reallege every allegation set forth in the preceding paragraphs.

147. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq*., the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

148. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard its customers' PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and class members from further data breaches that compromise their PII. Plaintiffs remain at imminent risk that further compromises of their PII will occur in the future.

149. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. Defendant continues to owe a legal duty to secure consumers' PII and to timely notify consumers of a data breach under the common law, Section 5 of the FTC Act, and various state statutes.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

b. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure consumers' PII.

150. The Court also should issue corresponding prospective injunctive relief requiring Defendant to employ adequate security practices consistent with law and industry standards to protect consumers' PII.

151. If an injunction is not issued, Plaintiffs and class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach occurs, Plaintiffs and class members will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

152. The hardship to Plaintiffs and class members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if another massive data breach occurs at T-Mobile, Plaintiffs and class members will likely be subjected to fraud, identify theft, and other harms described herein. On the other hand, the cost to Defendant of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

153. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at T-Mobile, thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose PII would be further compromised.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

WHEREFORE, Plaintiffs demand a trial by jury and hereby respectfully request:

(a) That the Court determine that Plaintiffs' claims are suitable for class treatment and certify the proposed Class pursuant to Fed. R. Civ. P. 23;

(b) That the Court appoint Plaintiffs as representatives of the Classes;

(c) That Plaintiffs' counsel be appointed as counsel for the Classes;

(d) That the Court award compensatory damages, punitive damages, statutory and civil penalties to Plaintiffs and the Classes as warranted by the CCPA and other applicable law;

(e) In the alternative, that the Court award nominal damages as permitted by law;

(f) That the Court award injunctive or other equitable relief that directs Defendant to provide Plaintiffs and the Classes with free credit monitoring and identity theft protection, and to implement reasonable security procedures and practices to protect customers' PII that conform to relevant federal and state guidelines and industry norms;

(g) That the Court award declaratory judgment in favor of Plaintiffs determining that Defendant's failure to implement reasonable security measures gives rise to a claim under the CCPA;

(h) That the Court award reasonable costs and expenses incurred in prosecuting this action, including attorneys' fees and expert fees pursuant to Cal. Code Civ. P. § 1021.5; and

(i) Such other relief as the Court may deem just and proper.

VIII. JURY DEMAND

Pursuant to Fed. R. Civ. P. 38(b), Plaintiffs demand a trial by jury of all issues properly triable to a jury in this case.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Dated: August 19, 2021

TOUSLEY BRAIN STEPHENS PLLC

By: */s/ Kim D. Stephens*
Kim D. Stephens, P.S., WSBA #11984
/s/ Jason T. Dennett
Jason T. Dennett, WSBA #30686
/s/ Kaleigh N. Powell
Kaleigh N. Powell, WSBA #52684
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600/Fax: (206) 682-2992
Email: jdennett@tousley.com
kstephens@tousley.com
kpowell@tousley.com

By: */s/ Daniel J. Mogin*
Daniel J. Mogin
MOGINRUBIN LLP
Daniel J. Mogin*
Jennifer M. Oliver*
Timothy Z. LaComb*
600 W. Broadway, Suite 3300
San Diego, CA 92101
Telephone: (619) 687-6611
Facsimile: (619) 687-6610
dmogin@moginrubin.com
joliver@moginrubin.com
tlacomb@moginrubin.com

Jonathan L. Rubin*
1615 M Street, NW, Third Floor
Washington, D.C. 20036
Tel: (202) 630-0616
Fax: (877) 247-8586
jrubin@moginrubin.com

Norman E. Siegel*
Barrett J. Vahle*
J. Austin Moore*
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
Telephone: (816) 714-7100
siegel@stuevesiegel.com
vahle@stuevesiegel.com
moore@stuevesiegel.com

James Pizzirusso*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, DC 20006
Telephone: 202-540-7200
jpizzirusso@hausfeld.com

Steven M. Nathan*
HAUSFELD LLP
33 Whitehall St., 14th Floor
New York, NY 10004
Telephone: (646) 357-1100
snathan@hausfeld.com

*Pro Hac Vice forthcoming

Attorneys for Plaintiffs

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992